IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

LAURIE GERBER, *on behalf of herself and all others similarly situated*, Plaintiff, v. CENCORA, INC. and THE LASH GROUP, LLC, Defendants.	Civil Action No. 24-2303 **CLASS ACTION COMPLAINT** **TRIAL BY JURY DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Laurie Gerber ("Plaintiff Gerber" or "Plaintiff") brings this Class Action Complaint against Cencora, Inc. ("Cencora") and the Lash Group, LLC ("Lash Group") (collectively, "Defendants"), individually and on behalf of all others similarly situated Class Members, and alleges, upon information and belief, and as to her own actions and her counsel's investigation, the following:

INTRODUCTION

1. Plaintiff brings this class action lawsuit against Defendants for their failure to properly secure and safeguard the personally identifiable information and personal health information ("PII" and "PHI") (collectively, "Private Information") for approximately half a million people.[1]

[1] https://www.theregister.com/2024/05/27/security_in_brief/ (last accessed May 29, 2024).

2. On February 21, 2024, Cencora "learned that data from its information systems had been exfiltrated, some of which may contain personal information" by an unauthorized third-party ("the Data Breach").[2]

3. Following an investigation of the Breach, Cencora determined that the incident compromised the PII and PHI of individuals taking part in the Bristol Myers Squibb Patient Assistance Foundation, including their names, addresses, dates of birth, health diagnoses, medications, and prescriptions.[3]

4. On February 27, 2024, Cencora filed an 8-K with the Securities and Exchange Commission in which Cencora disclosed:

> On February 21, 2024, Cencora, Inc. (the "Company"), learned that data from its information systems had been exfiltrated, some of which may contain personal information. Upon initial detection of the unauthorized activity, the Company immediately took containment steps and commenced an investigation with the assistance of law enforcement, cybersecurity experts, and external counsel.
>
> As of the date of this filing, the incident has not had a material impact on the Company's operations, and its information systems continue to be operational. The Company has not yet determined whether the incident is reasonably likely to materially impact the Company's financial condition or results of operations.[4]

5. In its 8-K disclosure, Cencora acknowledges that Plaintiff's and Class Members' Private Information had been unlawfully accessed and exfiltrated.

6. Despite announcing the Data Breach at the end of February 2024, Cencora did not begin sending out notice to impacted individuals until late May 2024.

7. Cencora has not yet disclosed details about the nature of the cyber-attack, what types of Private Information were compromised, or the number of individuals impacted.

---

[2] https://www.sec.gov/ix?doc=/Archives/edgar/data/1140859/000110465924028288/tm247267d1_8k.htm (last accessed May 29, 2024).

[3] https://www.teiss.co.uk/news/pharmaceuticals-firm-cencora-says-data-breach-impacted-bristol-myers-squibb-customers-14073 (last accessed May 29, 2024).

[4] https://www.sec.gov/ix?doc=/Archives/edgar/data/1140859/000110465924028288/tm247267d1_8k.htm (last accessed May 29, 2024).

8. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Cencora's inadequate safeguarding of Plaintiff's and Class Members' Private Information.

PARTIES

Plaintiff Gerber

9. Plaintiff Laurie Gerber ("Plaintiff Gerber" or "Plaintiff") is an adult and a resident of the State of New York.

10. Plaintiff Gerber resides in Suffolk County, New York.

11. On or around May 17, 2024, Plaintiff Gerber received a Notice of Data Security Incident ("the Notice") from Defendants informing her that her Private Information had been involved in the Data Breach.[5]

12. Plaintiff Gerber is deeply concerned about protecting her Private Information from public disclosure. Consequently, Plaintiff Gerber is deeply shocked and concerned about the Data Breach, especially since it involves her sensitive PII and PHI.

13. Since the announcement of the Data Breach, Plaintiff Gerber has been required to spend her valuable time researching the Data Breach and determining exactly what Private Information was involved.

14. As a result of the Data Breach, Plaintiff Gerber will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

Defendant Cencora, Inc.

15. Defendant Cencora, Inc. ("Cencora") is a Delaware company with its principal place of business located at 1 West First Avenue, Conshohocken, PA 19428-1800.

16. Cencora is a pharmaceutical services company that provides distribution solutions

[5] Notice of Data Security Incident, *supra.* 1

for doctor's offices and pharmacies, and animal healthcare.[6]

Defendant Lash Group, LLC

17. Defendant the Lash Group, LLC ("Lash Group") is a company with its principal place of business located at 1 West First Avenue, Conshohocken, PA 19428-1800. Lash Group is a patient support company, owned by Defendant Cencora, that provides patient support services, business analytics and technology services, and other services to pharmaceutical companies, pharmacies, and other healthcare providers.[7]

JURISDICTION & VENUE

18. This court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendants, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

19. This Court has personal jurisdiction over Defendants because they operate and are headquartered in this District and conduct substantial business in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendants are based in this District, maintain Plaintiff's and Class Members' Private Information in this District, and have caused harm to Plaintiff and Class Members in this District.

[6] https://www.cencora.com/who-we-are/history (last accessed May 29, 2024).
[7] https://www.lashgroup.com/who-we-are (last accessed May 29, 2024).

FACTUAL ALLEGATIONS

21. Cencora is a Pennsylvania-based pharmaceutical services company that provides distribution solutions for doctor's offices, pharmacies, and animal healthcare.

22. Formerly known as AmeriSourceBergen until 2023, Cencora handles around 20% of the pharmaceuticals sold and distributed throughout the United States.

23. As a condition for providing services, Cencora requires its clients to entrust it with their Private Information.

24. Upon information and belief, Cencora collects and maintains the Private Information of its clients, including, but not limited to: name; address; phone number; email address; date of birth; demographic information; information relating to individual medical history; information concerning an individual's doctor, nurse, or other medical providers; medical information; health insurance information; phone identification; and other information that Cencora may deem necessary to provide its services.

25. Due to the highly sensitive and personal nature of the information Cencora acquires and stores with respect to its clients, Plaintiff and Class Members reasonably expect that Cencora will; keep their Private Information confidential; comply with industry standards related to data security and Private Information; inform them of legal duties and comply with all federal and state laws protecting their Private Information; only use and release their Private Information for reasons that relate to providing services; and provide adequate notice to them if their Private Information is disclosed without authorization.

26. Plaintiff and Class Members entrusted Cencora with their Private Information but, contrary to Cencora's duties, promises, and the reasonable expectations of Plaintiff and Class Members, Cencora implemented substandard data security practices and failed to adhere to industry standard practices. Not only did Cencora maintain inadequate security to protect its

systems from infiltration by cybercriminals, but it waited nearly three months to notify impacted individuals like Plaintiff and Class Members about the Data Breach.

A. The Data Breach

27. According to Cencora's 8-K Filing, on February 21, 2024, Cencora learned that it was subject to a cybersecurity attack but did not reveal when the attack occurred.[8]

28. Cencora discovered that the Data Breach may have impacted Private Information stored in its systems and encrypted files.

29. Cencora stated: "[u]pon initial detection of the unauthorized activity, the Company immediately took containment steps and commenced an investigation with the assistance of law enforcement, cybersecurity experts and external counsel."[9]

30. Cencora did not begin sending out letters to impacted individuals until the week of May 20, 2024. In its letters, Cencora said the data from its systems includes patient names, their postal address and date of birth, as well as information about their diagnoses and medications.[10]

31. As an entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk of which Cencora was aware and knew it had a duty to guard against.

B. Defendants Failed to Comply with FTC Guidelines

32. Defendants were prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal

[8] https://www.sec.gov/ix?doc=/Archives/edgar/data/1140859/000110465924028288/tm247267d1_8k.htm (last accessed May 29, 2024).
[9] *Id.*
[10] https://techcrunch.com/2024/05/24/cencora-americans-health-data-stolen-breach-cyberattack/ (last accessed May 29, 2024).

information is an "unfair practice" in violation of the FTC Act. See, e.g., FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

33. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

34. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[11] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[12]

35. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

36. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as

[11] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed May 29, 2024).
[12] *Id.*

an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

37. These FTC enforcement actions include actions against healthcare providers and partners like Defendants. See, e.g., In the Matter of LabMD, Inc., A Corp, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

38. Defendants failed to properly implement basic data security practices.

39. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to customer's Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

40. Defendants were at all times fully aware of the obligation to protect the Private Information of customers and patients. Defendants were also aware of the significant repercussions that would result from their failure to do so.

C. The Healthcare Sector is Particularly Vulnerable to Cyber Attacks

41. Defendants were on notice that companies in the healthcare industry are targets for data breaches.

42. Defendants were on further notice regarding the increased risks of inadequate cybersecurity. In February 2022, the cybersecurity arm of the U.S. Department of Health and Human Services ("HHS") issued a warning to hospitals and healthcare systems about a dramatic rise in cyberattacks, urging facilities to shore up their cyber defenses.[13] Indeed, just

[13] Rebecca Pifer, *Tenet says 'cybersecurity incident' disrupted hospital operations*, HEALTHCAREDIVE (Apr. 26, 2022), https://www.healthcaredive.com/news/tenet-says-cybersecurity-incident-disrupted-hospital-operations/622692/. (last accessed May 29, 2024).

days before, HHS's cybersecurity arm issued yet another warning about increased cyberattacks that urged vigilance with respect to data security.[14]

43. In the context of data breaches, healthcare is "by far the most affected industry sector."[15] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[16] A Tenable study analyzing publicly disclosed healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in *nearly 93% of the breaches*."[17]

44. Defendants were also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[18]

45. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial

---

[14] *Id.* (HHS warned healthcare providers about the increased potential for attacks by a ransomware group called Hive, "[c]alling it one of the 'most active ransomware operators in the cybercriminal ecosystem,' the agency said reports have linked Hive to attacks on 355 companies within 100 days of its launch last June — nearly three a day.").

[15] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed March 28, 2024).

[16] *See id.*

[17] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches. (last accessed May 28, 2024).

[18] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at*: https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last accessed May 28, 2024).

information, but also patient access to care.[19]

46. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[20] In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.[21] That trend continues.

47. The healthcare sector consistently reports one of the highest number of breaches among all measured sectors, with the highest rate of exposure per breach.[22] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[23] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[24]

48. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients

---

[19] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last accessed May 28, 2024).
[20] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at:* https://www.idtheftcenter.org/surveys-studys (last accessed May 28, 2024).
[21] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review, available at:* https://www.idtheftcenter.org/2017-data-breaches/ (last accessed May 28, 2024).
[22] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last accessed May 28, 2024).
[23] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed May 28, 2024).
[24] *Id.*

at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[25]

D. Defendants Acquire, Collect, and Store Plaintiff's and Class Members' Private Information

49. In the course of its regular business operations, Defendants acquired, collected, and stored Plaintiff's and Class Members' Personal Information.

50. As a condition of its relationships with Plaintiff and Class Members and Defendant's clients, Defendants required that Plaintiff and Class Members entrust Defendants with highly confidential PII.

51. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Personal Information from disclosure.

52. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Personal Information and relied on Defendants to keep their Personal Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

53. Yet, despite the prevalence of public announcements of these data breach and data security compromises, Defendants failed to take appropriate steps to protect Plaintiff's and Class Members' Personal Information from being compromised.

E. Securing Private Information and Preventing Breaches

54. Defendants could have prevented this Data Breach by properly securing its networks and encrypting the Personal Information of Plaintiff and Class Members. Alternatively, Defendants could have destroyed the data, especially decade-old data from

[25] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks. (last accessed May 28, 2024).

former patients or employees.

55. Defendants' negligence in safeguarding the Personal Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

56. Indeed, despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Personal Information of Plaintiff and Class Members from being compromised.

57. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[26] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[27]

58. The ramifications of Defendants' failure to keep secure the Personal Information of Plaintiff and Class Members are long lasting and severe. Once stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

F. Value of Private Information

59. The Personal Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price

[26] 17 C.F.R. § 248.201 (2013).
[27] *Id*.

ranging from $40 to $200, and bank details have a price range of $50 to $200.[28] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[29] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[30]

60. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[31]

61. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

62. Even then, a new Social Security number may not be effective. According to

---

[28] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed May 28, 2024).

[29] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed May 28, 2024).

[30] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed May 28, 2024).

[31] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed May 28, 2024).

Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[32]

63. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, Social Security number, and potentially date of birth.

64. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[33]

65. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

66. The Personal Information of Plaintiff and Class Members was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the Personal Information for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

67. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

---

[32] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed May 28, 2024).

[33] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed May 28, 2024).

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[34]

68. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Personal Information of Plaintiff and Class Members, including Social Security numbers and/or dates of birth, and of the foreseeable consequences that would occur if the Personal Information was compromised, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members a result.

69. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their Personal Information.

70. Defendants were, or should have been, fully aware of the unique type and the significant volume of data stored on and/or shared on its system and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

71. To date, Defendants have offered credit monitoring services only "for twelve months from the date of enrollment when changes occur to your credit file."[35]

72. Further, there is a market for Plaintiff's and Class Members PHI, and the stolen PHI has inherent value.

73. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements.

---

[34] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/products/gao-07-737 (last accessed May 28, 2024).

[35] https://oag.ca.gov/system/files/MD%20-%20Letter%20to%20Patients%20%28general%29%20-%20Redacted%20Proof%284085005.1%29.pdf (last accessed May 28, 2024).

It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

74. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[36]

75. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Personal Information of Plaintiff and Class Members.

G. Defendants' Conduct Violates the Rules and Regulations of HIPAA and HITECH

76. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendants left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

[36] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, Kaiser Health News (Feb. 7, 2014), *available at* https://khn.org/news/rise-of-indentity-theft/ (last accessed May 28, 2024).

77. Defendants are covered entities pursuant to HIPAA. *See* 45 C.F.R. § 160.102. Defendants must therefore comply with the HIPAA Privacy Rule and Security Rule. See 45 C.F.R. Part 160 and Part 164, Subparts A through E.

78. Defendants are covered entities pursuant to the Health Information Technology Act ("HITECH").[37] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

79. Plaintiff's and Class Members' Personal Information is "protected health information" as defined by 45 CFR § 160.103.

80. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

81. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

82. Plaintiff's and Class Members' Personal Information is "unsecured protected health information" as defined by 45 CFR § 164.402.

83. Plaintiff's and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

84. Plaintiff's and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

[37] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

85. Plaintiff's and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

86. Plaintiff's and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

87. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

88. The Data Breach could have been prevented if Defendants implemented HIPAA mandated, industry standard policies and procedures for securely disposing of Personal Information when it was no longer necessary and/or had honored its obligations to Plaintiff and Class Members.

89. It can be inferred from Defendants' Data Breach that Defendants either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiff and Class Members' Personal Information.

90. Defendants' security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendants create, receive, maintain, and transmit in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendants' workforce in violation of 45 CFR 164.306(a)(94);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502,et seq.; and

k. Retaining information past a recognized purpose and not deleting it.

91. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendants to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

92. Because Defendants have failed to comply with industry standards, while monetary relief may cure some of Plaintiff and Class Members' injuries, injunctive relief is necessary to ensure Defendants' approach to information security is adequate and appropriate. Defendants still maintain the Personal Information of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Plaintiff's and Class Members' Personal Information remains at risk of subsequent data breaches.

CLASS ACTION ALLEGATIONS

93. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3), *et seq.* and other applicable law.

94. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> ***All persons whose Private Information was compromised in the Data Breach that was discovered by Cencora on or around February 21, 2024.***

95. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have controlling interests; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

96. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

97. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant class-wide relief because Plaintiff

and all members of the Nationwide Class were subjected to the same wrongful practices by Defendants, entitling them to the same relief.

98. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Federal Rule of Civil Procedure 23.

99. The Nationwide Class is so numerous that individual joinder of its members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, Plaintiff is informed and believes that there are at least thousands of Class Members.

100. Common questions of law and fact exist as to members of the Nationwide Class and predominate over any questions which affect only individual members of the Class. These common questions include, but are not limited to:

a. Whether and to what extent Defendants had a duty to protect the Personal Information of Plaintiff and Class Members;

b. Whether Defendants had a duty not to disclose the Personal Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendants had a duty not to use the Personal Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the Personal Information of Plaintiff and Class Members;

e. Whether and when Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their Personal Information had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their Personal Information had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information

compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Personal Information of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

101. Plaintiff is a member of the Classes he seeks to represent, and her claims and injuries are typical of the claims and injuries of the other Class Members.

102. Plaintiff will adequately and fairly protect the interests of other Class Members. Plaintiff has no interests adverse to the interests of absent Class Members. Plaintiff is represented by legal counsel with substantial experience in class action litigation. The interests of Class Members will be fairly and adequately protected by Plaintiff and her counsel.

103. Defendants have acted or refused to act on grounds that apply generally to the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

104. A class action is superior to other available means for fair and efficient adjudication

of the claims of the Class and would be beneficial for the parties and the court. Class action treatment will allow a large number of similarly situated persons to prosecute their common claims in a single forum, simultaneously, efficiently, and without the unnecessary duplication

of effort and expense that numerous individual actions would require. The amounts owed to the many individual Class Members are likely to be relatively small, and the burden and expense of individual litigation would make it difficult or impossible for individual members of the class to seek and obtain relief. A class action will serve an important public interest by permitting such individuals to effectively pursue recovery of the sums owed to them. Further, class litigation prevents the potential for inconsistent or contradictory judgments raised by individual litigation. Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

COUNT 1
Negligence
(On Behalf of the Plaintiff and the Nationwide Class)

105. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 98.

106. Plaintiff and the Nationwide Class provided and entrusted Defendants with certain Personal Information as a condition of receiving medical services and care based upon the premise and with the understanding that Defendants would safeguard their information, use their Personal Information for business purposes only, and/or not disclose their Personal Information to unauthorized third parties.

107. Defendants have full knowledge of the sensitivity of the Personal Information and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the Personal Information were wrongfully disclosed.

108. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Personal Information of Plaintiff and the Nationwide Class involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

109. Defendants had a duty to exercise reasonable care in safeguarding,

securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the Personal Information of Plaintiff and the Nationwide Class in Defendants' possession was adequately secured and protected.

110. Defendants owed a duty to Plaintiff and the Nationwide Class to implement intrusion detection processes that would detect a data breach or unauthorized access to its systems in a timely manner.

111. Defendants also had a duty to exercise appropriate clearinghouse practices to remove Personal Information they were no longer required to retain pursuant to regulations, including that of former customers.

112. Defendants also had a duty to employ proper procedures to detect and prevent the improper access, misuse, acquisition, and/or dissemination of the Personal Information of Plaintiff and the Nationwide Class.

113. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and the Nationwide Class. That special relationship arose because Plaintiff and the Nationwide Class entrusted Defendants and Defendants' clients with their confidential Personal Information, a necessary part of their relationships with Defendants.

114. Defendants owed a duty to disclose the material fact that Defendants' data security practices were inadequate to safeguard the personal and medical information of Plaintiff and the Nationwide Class.

115. Defendants' Privacy Policies acknowledge Defendants' duty to adequately protect the personal and medical information of Plaintiff and the Nationwide Class.

116. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

117. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the Personal Information of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that Personal Information, and the necessity for encrypting Personal Information stored on Defendants' systems.

118. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendants' misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included its decisions not to comply with industry standards for the safekeeping of the Personal Information of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendants.

119. Plaintiff and the Nationwide Class had no ability to protect their Personal Information that was in, and likely remains in, Defendants' possession.

120. Defendants were in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

121. Defendants had and continue to have a duty to adequately disclose that the Personal Information of Plaintiff and the Nationwide Class within Defendants' possession was compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Personal Information by third parties.

122. Defendants have admitted that the Personal Information of Plaintiff and the Nationwide Class was wrongfully accessed, acquired, and/or released to unauthorized third persons as a result of the Data Breach.

123. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Personal Information of Plaintiff and the Nationwide Class during the time the Personal Information was within Defendants' possession or control.

124. Defendants improperly and inadequately safeguarded the Personal Information of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

125. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the Personal Information of Plaintiff and the Nationwide Class in the face of increased risk of theft.

126. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect unauthorized access or intrusions and prevent dissemination of their Personal Information. Additionally, Defendants failed to disclose to Plaintiff and the Nationwide Class that Defendants' security practices were inadequate to safeguard the Personal Information of Plaintiff and the Nationwide Class.

127. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove Personal Information it was no longer required to retain pursuant to regulations, including Personal Information of former patients and employees.

128. Defendants, through their actions and/or omissions, unlawfully breached

their duty to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Data Breach.

129. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the Personal Information of Plaintiff and the Nationwide Class would not have been compromised.

130. There is a close causal connection between Defendants' failure to implement security measures to protect the Personal Information of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The Personal Information of Plaintiff and the Nationwide Class was accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such Personal Information by adopting, implementing, and maintaining appropriate security measures.

131. As a direct and proximate result of Defendants' negligence, Plaintiff and the Nationwide Class have suffered and will continue to suffer injury.

132. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their Personal Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

133. As a direct and proximate result of Defendants' negligence, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT 2
Negligence Per Se
(On Behalf of the Plaintiff and the Nationwide Class)

134. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 98.

135. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

136. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Nationwide Class.

137. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

138. Plaintiff and the Nationwide Class are within the class of persons that the FTC Act was intended to protect.

139. The harm that occurred because of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Nationwide Class.

140. Defendants' violations of HIPAA and HITECH also independently constitute negligence *per se*.

141. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

142. Plaintiff and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

143. The harm that occurred because of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

144. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Personal Information is used; iii) the compromise, publication, and/or theft of their Personal Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Personal Information, which remain in Defendants' possession and are subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Personal Information of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the

remainder of the lives of Plaintiff and the Nationwide Class.

COUNT 3
Breach of Implied Contract
(On Behalf of the Plaintiff and the Nationwide Class)

145. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 98.

146. Defendants required Plaintiff and the Nationwide Class to provide and entrust their Personal Information as a condition of obtaining medical care from Defendants' clients.

147. Plaintiff and the Nationwide Class paid money to Defendants in exchange for goods and services, as well as Defendants' promises to protect their protected health information and other Personal Information from unauthorized disclosure.

148. Defendants promised to comply with HIPAA and HITECH standards and to make sure that Plaintiff's and Class Members' Personal Information would remain protected.

149. As a condition of obtaining medical care from Defendants' clients , Plaintiff and the Nationwide Class provided and entrusted their personal information. In so doing, Plaintiff the Nationwide Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Nationwide Class if their data had been breached and compromised or stolen.

150. A meeting of the minds occurred, as Plaintiff and Class Members agreed, *inter alia*, to provide accurate and complete Personal Information and to pay Defendants in exchange for Defendants' agreement to, *inter alia*, protect their Personal Information.

151. Plaintiff and the Nationwide Class Members would not have entrusted their Personal Information to Defendants in the absence of Defendants' implied promise to adequately safeguard this confidential personal and medical information.

152. Plaintiff and the Nationwide Class fully performed their obligations under the

implied contracts with Defendants.

153. Defendants breached the implied contracts it made with Plaintiff and the Nationwide Class by making their Personal Information accessible from the internet (regardless of any mistaken belief that the information was protected) and failing to make reasonable efforts to use the latest security technologies designed to help ensure that the Personal Information was secure, failing to encrypt Plaintiff and Class Members' sensitive Personal Information, failing to safeguard and protect their Personal Information, and by failing to provide timely and accurate notice to them that Personal Information was compromised as a result of the data breach.

154. Defendants further breached the implied contracts with Plaintiff and Class Members by failing to comply with their promise to abide by HIPAA and HITECH.

155. Defendants further breached the implied contracts with Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendants created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

156. Defendants further breached the implied contracts with Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

157. Defendants further breached the implied contracts with Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

158. Defendants further breached the implied contracts with Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate,

to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

159. Defendants further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

160. Defendants further breached the implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

161. Defendants further breached the implied contracts with Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations in violation of 45 CFR 164.306(a)(94).

162. Defendants further breached the implied contracts with Plaintiff and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*.

163. Defendants further breached the implied contracts with Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

164. Defendants further breached the implied contracts with Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Personal Information.

165. Defendants' failures to meet these promises constitute breaches of the implied contracts.

166. Because Defendants allowed unauthorized access to Plaintiff and Class Members' Personal Information and failed to safeguard the Personal Information, Defendants breached their contracts with Plaintiff and Class Members.

167. Defendants breached their contracts by not meeting the minimum level of protection of Plaintiff and Class Members' protected health information and other Personal Information, because Defendants did not prevent against the breach.

168. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Defendants providing goods and services to Plaintiff and Class Members that were of a diminished value.

169. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and the Nationwide Class are now subject to the present and continuing risk of fraud, and are suffering (and will continue to suffer) the ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the diminished value of services provided by Defendants; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

170. As a result of Defendants' breach of implied contract, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT 4
Breach of Fiduciary Duty
(On Behalf of the Plaintiff and the Nationwide Class)

171. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 98.

172. Plaintiff and Class Members either directly or indirectly gave Cencora and Lash Group their Private Information in confidence, believing that Cencora and Lash Group – healthcare organizations – would protect that information. Plaintiff and Class Members would not have provided Cencora and Lash Group with this information had they known it would not be adequately protected. Cencora's and Lash Group's acceptance and storage of Plaintiff's and Class Members' Private Information created a fiduciary relationship between Defendants and Plaintiff and Class Members. In light of this relationship, Cencora and Lash Group must act primarily for the benefit of its patients (at least insofar as it relates to the safeguarding of their PII).

173. Cencora has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' Private Information, failing to comply with the data security guidelines set forth by Section 5 of the FTCA, and otherwise failing to safeguard the Private Information of Plaintiff and Class Members it collected.

174. As a direct and proximate result of Cencora's and Lash Group's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual

and future consequences of the Data Breach; (v) the continued risk to their Private Information which remains in Cencora's and Lash Group's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT 5
Unjust Enrichment
(On Behalf of the Plaintiff and the Nationwide Class)

175. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 98.

176. Plaintiff and Class Members conferred a monetary benefit upon Cencora and Lash Group in the form of monies paid for educational services or other services.

177. Cencora and Lash Group accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class Members. Cencora and Lash Group also benefited from the receipt of Plaintiff's and Class Members' Private Information.

178. As a result of Cencora's and Lash Group's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

179. Cencora and Lash Group should not be permitted to retain the money belonging to Plaintiff and Class Members because Cencora failed to adequately implement the data privacy and security procedures for themselves self that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards.

180. Cencora and Lash Group should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of herself and all others similarly situated, prays for relief as follows:

(a) For an order certifying the class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

(b) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(c) For damages, including compensatory, punitive, and/or nominal damages, in an amount to be determined by the trier of fact;

(d) For an order of restitution and all other forms of equitable monetary relief;

(e) Declaratory and injunctive relief as described herein;

(f) Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses;

(g) Awarding pre- and post-judgement interest on any amounts awarded; and

(h) Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

Date: May 30, 2024

Respectfully submitted,

LAURIE GERBER, *on behalf of herself and all others similarly situated*,

By: */s/ James A. Francis*

James A. Francis
FRANCIS MAILMAN SOUMILAS, P.C.
1600 Market Street, Suite 2510
Philadelphia, PA 19103
Tel: (215) 735-8600
Fax: (215) 940-8000
jfrancis@consumerlawfirm.com

Jennifer Czeisler*
Edward Ciolko*
Sterlington, PLLC
One World Trade Center
85th Floor
New York, NY 10007
(516) 457-9571
jen.czeisler@sterlingtonlaw.com
edward.ciolko@sterlingtonlaw.com

Attorneys for Plaintiff

**Pro Hac Vice application forthcoming*